CLAIMS

1. A method for enabling integrity checking of a software
module to be used in a mobile communication terminal,
said terminal capable of communicating in a mobile
5   communication system, said software module being stored
on a removable memory unit connected to the terminal,
said method c h a r a c t e r i z e d in that the terminal
communicates via the mobile communication system with the
software provider, said communication including reception
10   of a digitally signed data block comprising a reference
value for use during integrity checking of said software
module.

2. A method according to claim 1, comprising the steps
of:
15   hashing the software module, resulting in a first
hash value,
         transmitting a first identifier, associated with
the memory unit, a second identifier, associated with the
terminal and the first hash value via the mobile
20   communication system to a provider of the software
module,
         receiving, from the provider of the software
module, a data block comprising a digital signature and
further data associated with the memory unit and the
25   terminal,
         analyzing the received data block, comprising
verification of the digital signature and comparison of
said further data with said first and second identifiers,
         storing the received data block comprising the
30   digital signature, thereby providing a reference value
for use during integrity checking of said software
module.

3. A method according to claim 2, where the transmission
of the first identifier includes transmission of a memory
35   unit serial number.

12

4. A method according to claim 2, where the transmission of the first identifier includes transmission of a software module identification number.

5. A method according to claim 2, where the transmission of the second identifier includes transmission of an international mobile station equipment identity code.

6. A mobile communication terminal, comprising means for enabling integrity checking of a software module to be used in the terminal, said terminal capable of communicating in a mobile communication system, said software module being stored on a removable memory unit connected to the terminal, said terminal c h a r a c t e r i z e d in that it comprises means for communicating via the mobile communication system with the software provider, said means for communication including means for receiving a digitally signed data block comprising a reference value for use in means for integrity checking of said software module.

7. A terminal according to claim 6, comprising:
    means for hashing the software module, arranged to provide a first hash value,
    means for transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to a provider of the software module,
    means for receiving, from the provider of the software module, a data block comprising a digital signature and further data associated with the memory unit and the terminal,
    means for analyzing the received data block, comprising means for verification of the digital signature and comparison of said further data with said first and second identifiers,
    means for storing the received data block comprising the digital signature, arranged to provide a

reference value for use during integrity checking of said software module.

8. A terminal according to claim 7, where the means for transmitting the first identifier includes means for transmitting a memory unit serial number.

9. A terminal according to claim 7, where the means for transmitting the first identifier includes means for transmitting a software module identification number.

10. A terminal according to claim 7, where the means for transmitting the second identifier includes means for transmitting an international mobile station equipment identity code.

14